CLAIMS

What is claimed is:

1. A method to reduce a search space for determining viable cellular automata based random number generators (CA-based RNGs), comprising:

counting number of 1s and 0s of outputs of a truth table for a candidate CA-based RNG;

counting number of 1s and 0s of inputs of said truth table for said candidate CA-based RNG; and

accepting or rejecting said candidate CA-based RNG based on results of said counting steps.

2. The method of claim 1, wherein in said step of accepting or rejecting said candidate CA-based RNG comprises:

accepting said candidate CA-based RNG in response to all of the following conditions being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table generating 1s for output is less than or equal to a predetermined 1s input difference threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table generating 0s for output is less than or equal to a predetermined 0s input difference threshold.

3. The method of claim 2, wherein at least one of said predetermined output difference threshold, predetermined 0s input difference threshold, and predetermined 1s input difference threshold is zero.

4. The method of claim 1, wherein in said step of accepting or rejecting said candidate CA-based RNG comprises:

rejecting said candidate CA-based RNG in response to at least one of the following conditions not being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table generating 1s for output is less than or equal to a predetermined 1s input difference threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table generating 0s for output is less than or equal to a predetermined 0s input difference threshold.

5. The method of claim 4, wherein at least one of said predetermined output difference threshold, predetermined 0s input difference threshold, and predetermined 1s input difference threshold is zero.

6. A system to reduce a search space for determining viable cellular automata based random number generator (CA-based RNGs), comprising:

a truth-table-counting-module counting number of 1s and 0s of outputs of a truth table for a candidate CA-based RNG, said truth-table-counting module also

counting number of 1s and 0s of inputs of said truth table for said candidate CA-based RNG; and

a prescreening-module accepting or rejecting said candidate CA-based RNG based on an output or outputs of said truth-table-counting module.

7. The system of claim 6, wherein said truth-table-counting-module comprises:

an output-counting-module counting number of 1s and 0s of said outputs of said truth table for said candidate CA-based RNG; and

an input-counting-module counting number of 1s and 0s of said inputs of said truth table for said candidate CA-based RNG.

8. The system of claim 6, wherein said prescreening-module accepts said candidate CA-based RNG accepts in response to all of the following conditions being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table generating 1s for output is less than or equal to a predetermined 1s input difference threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table generating 0s for output is less than or equal to a predetermined 0s input difference threshold.

9. The system of claim 8, wherein at least one of said predetermined output difference threshold, predetermined 0s input difference threshold, and predetermined 1s input difference threshold is zero.

10. The system of claim 6, wherein in said prescreening-module accepts said candidate CA-based RNG rejects in response to at least one of the following conditions not being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table generating 1s for output is less than or equal to a predetermined 1s input difference threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table generating 0s for output is less than or equal to a predetermined 0s input difference threshold.

11. The system of claim 10, wherein at least one of said predetermined output difference threshold, predetermined 0s input difference threshold, and predetermined 1s input difference threshold is zero.

12. A computer readable medium on which is embedded computer software comprising a set of instructions for performing a method to reduce a search space for determining viable cellular automata based random number generator (CA-based RNGs), said method comprising:

counting number of 1s and 0s of outputs of a truth table for a candidate CA-based RNG;

counting number of 1s and 0s of inputs of said truth table for said candidate CA-based RNG; and

accepting or rejecting said candidate CA-based RNG based on results of said counting steps.

13. The computer readable medium of claim 12, wherein in said method (200), said step of accepting or rejecting said candidate CA-based RNG comprises:

accepting said candidate CA-based RNG in response to all of the following conditions being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table generating 1s for output is less than or equal to a predetermined 1s input difference threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table generating 0s for output is less than or equal to a predetermined 0s input difference threshold.

14. The computer readable medium of claim 13, wherein at least one of said predetermined output difference threshold, predetermined 0s input difference threshold, and predetermined 1s input difference threshold is zero.

15. The computer readable medium of claim 12, wherein in said method, said step of accepting or rejecting said candidate CA-based RNG comprises:

rejecting said candidate CA-based RNG in response to at least one of the following conditions not being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table generating 1s for output is less than or equal to a predetermined 1s input difference threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table generating 0s for output is less than or equal to a predetermined 0s input difference threshold.

16. The computer readable medium of claim 15, wherein at least one of said predetermined output difference threshold, predetermined 0s input difference threshold, and predetermined 1s input difference threshold is zero.